

#2
BT

Atty. Dkt. No. 068398-010702-6-03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Virgil D. GLIGOR et al.

Title: PARALLEL BLOCK ENCRYPTION METHOD
AND MODES FOR DATA CONFIDENTIALITY
AND INTEGRITY PROTECTION

Appl. No.: 09/931,151

Filing Date: 08/17/2001

Examiner: Unassigned

Art Unit: 2131

RECEIVED
JAN 31 2003
Technology Center 2100**INFORMATION DISCLOSURE STATEMENT**
UNDER 37 CFR §1.56Commissioner for Patents
Box PATENT APPLICATION
Washington, D.C. 20231

Sir:

Submitted herewith on Form PTO/SB/08 is a listing of documents known to Applicants in order to comply with Applicants' duty of disclosure pursuant to 37 CFR §1.56. A copy of each listed document is being submitted to comply with the provisions of 37 CFR §1.97 and §1.98.

The submission of any document herewith, which is not a statutory bar, is not intended as an admission that such document constitutes prior art against the claims of the present application or that such document is considered material to patentability as defined in 37 CFR §1.56(b). Applicants do not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference any document which is determined to be a *prima facie* art reference against the claims of the present application.

TIMING OF THE DISCLOSURE

The listed documents are being submitted in compliance with 37 CFR §1.97(b), before the mailing date of the first Office Action on the merits.

RELEVANCE OF EACH DOCUMENT

Excluding Document A7, the relevance of the documents are described in the present application.

Documents A7, A10, and A11 were cited in the International Search Report in Applicants' International Application PCT/US01/25949. A copy of the International Search Report setting forth the portion of each reference considered relevant by the Examiner is attached.

All of the documents are in English.

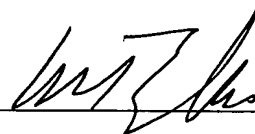
Applicants respectfully request that any listed document be considered by the Examiner and be made of record in the present application and that an initialed copy of Form PTO/SB/08 be returned in accordance with MPEP §609.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 CFR §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

Respectfully submitted,

Date January 30 ,2003

By



FOLEY & LARDNER
Customer Number: 22428



22428

PATENT TRADEMARK OFFICE

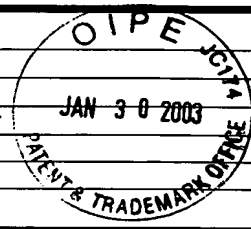
Telephone: (202) 672-5485

Facsimile: (202) 672-5399

William T. Ellis
Attorney for Applicant
Registration No. 26,874

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT Date Submitted: January 30, 2003 <i>(use as many sheets as necessary)</i>			Complete if Known		
Sheet	1	of	2	Application Number Filing Date First Named Inventor Group Art Unit Examiner Name Attorney Docket Number	09/931,151 08/17/2001 Virgil Dorin Gligor 2131 Unassigned 068398-0107



U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code ² (if known)			
	A1	5,757,913		BELLARE et al.	05/26/1998	
						RECEIVED JAN 31 2003

FOREIGN PATENT DOCUMENTS							Technology Center 2100	
Examiner Initials*	Cite No. ¹	Foreign Patent Document			Name of Patentee or Applicant of Cited Documents	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Office ³	Number ⁴	Kind Code ⁵ (if known)				

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ⁶
	A2	BELLARE et al., "A Concrete Security Treatment of Symmetric Encryption", <u>Proceedings of the 38th Symposium on Foundations of Computer Science</u> , 1997, pages 394-403, IEEE.	
	A3	BELLARE et al., "Keying Hash Functions for Message Authentication", <u>Advances in Cryptology- Crypto '96 Proceedings</u> , June 1996, pages 1-15, Lecture Notes in Computer Science Vol. 1109, Springer-Verlag.	
	A4	BELLARE et al., "XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions", <u>Advances in Cryptology- Crypto 95 Proceedings</u> , October 1995, pages 15-28, Lecture Notes in Computer Science Vol. 963, Springer-Verlag.	
	A5	BLACK et al., "UMAC: Fast and Secure Message Authentication", <u>Advances in Cryptology- Crypto '99</u> , 1999, pages 216-233, Lecture Notes in Computer Science Vol. 1666, Springer-Verlag.	
	A6	CAMPBELL, "Design and Specification of Cryptographic Capabilities", <u>Computer Security and the Data Encryption Standard</u> , February 1978, pages 54-66, National Bureau of Standards Special Publications 500-27, U.S. Department of Commerce.	
	A7	GLIGOR et al., "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes", October 27, 2000, pages 1-30, VDG Inc., Chevy Chase, Maryland, XP-002178464.	
	A8	GLIGOR et al., "Object Migration and Authentication", <u>IEEE Transactions on Software Engineering</u> , November 1979, pages 607-611, Vol. SE-5, No. 6., IEEE.	
	A9	GOLDWASSER et al., "Lecture Notes on Cryptography", August 1999, pages 1-10, 57-63 and 79-104, Cambridge, Massachusetts, http://www-cse.ucsd.edu/users/mihir/papers/gb.pdf .	
	A10	JUENEMAN et al., "Message Authentication with Manipulation Detection Codes", <u>Proceedings IEEE Symposium on Security and Privacy</u> , April 25, 1983, pages 33-54, XP-002055686.	

Examiner Signature	Date Considered	
--------------------	-----------------	--


*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² See attached Kinds of U.S. Patent Documents. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.

⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, D.C. 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO		Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	09/931,151	
Date Submitted: January 30, 2003		Filing Date	08/17/2001	
(use as many sheets as necessary)		First Named Inventor	Virgil Dorin Gligor	
Sheet 2 of 2		Group Art Unit	2131	
		Examiner Name	Unassigned	
		Attorney Docket Number	068398-0107	

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ⁶
	A11	JUTLA, "Encryption Modes with Almost Free Message Integrity", <u>Advances in Cryptology- EUROCRYPT 2001</u> , May 10, 2001, pages 529-544, Lecture Notes in Computer Science Vol. 2045, Springer-Verlag, Berlin, XP-002214999.	
	A12	KNUTH, <u>The Art of Computer Programming- Volume 2: Seminumerical Algorithms</u> , 1981, Chapter 3, Addison-Wesley.	
	A13	MENEZES et al., <u>Handbook of APPLIED CRYPTOGRAPHY</u> , 1997, Chapter 9, CRC Press LLC, Boca Raton.	
	A14	NAOR et al., "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs", <u>Advances in Cryptology- CRYPTO '98</u> , August 1998, pages 267-282, , Lecture Notes in Computer Science Vol. 1462, Springer-Verlag, Berlin.	
	A15	NATIONAL BUREAU of STANDARDS, "DES Modes of Operation", <u>FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION</u> , December 2, 1980, pages 1-26, Vol. 81, U.S. DEPARTMENT OF COMMERCE.	

RECEIVED

JAN 31 2003

Technology Center 2100

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² See attached Kinds of U.S. Patent Documents. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.

⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, D.C. 20231.